

2009 IEEE International Workshop on Hardware-Oriented Security and Trust

(HOST 2009)

**San Francisco, California, USA
27 July 2009**



**IEEE Catalog Number: CFP09HOA-PRT
ISBN: 978-1-4244-4805-0**

TABLE OF CONTENTS

Local Heating Attacks on Flash Memory Devices	1
<i>S. Skorobogatov</i>	
Fault Analysis of GRAIN-128	7
<i>A. Berzati, C. Canovas, G. Castagnos, B. Debraize, L. Goubin, A. Gouget, P. Paillier, S. Salgado</i>	
Security Evaluation of Different AES Implementations Against Practical Setup Time Violation Attacks in FPGAs	15
<i>S. Bhasin, N. Selmane, S. Guilley, J. Danger</i>	
Reconfigurable Physical Unclonable Functions – Enabling Technology for Tamper-Resistant Storage	22
<i>K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, P. Tuyls</i>	
Circuit-Level Techniques for Reliable Physically Unclonable Functions	30
<i>V. Vivekraj, L. Nazhandali</i>	
Temperature-Aware Cooperative Ring Oscillator PUF	36
<i>C. Yin, G. Qu</i>	
Robust Stable Radiometric Finger Printing for Wireless Devices	43
<i>A. Candore, O. Kocabas, F. Koushanfar</i>	
Experiences in Hardware Trojan Design and Implementation	50
<i>Y. Jin, N. Kupp, Y. Makris</i>	
Performance of Delay-Based Trojan Detection Techniques Under Parameter Variations	58
<i>D. Rai, J. Lach</i>	
New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time	66
<i>H. Salmani, M. Tehranipoor, J. Plusquellic</i>	
Analysis and Design of Active IC Metering Schemes	74
<i>R. Maes, D. Schellekens, P. Tuyls, I. Verbauwhede</i>	
Secure IP-Block Distribution for Hardware Devices	82
<i>J. Guajardo, T. Guney, S. S. Kumar, C. Paar</i>	
Early Feedback on Side-Channel Risks with Accelerated Toggle-Counting	90
<i>Z. Chen, P. Schaumont</i>	
Security Through Obscurity: An Approach for Protecting Register Transfer Level Hardware IP	96
<i>R. S. Chakraborty, S. Bhunia</i>	
OS Support for Detecting Trojan Circuit Attacks	100
<i>G. Bloom, B. Narahari, R. Simha</i>	
VITAMIN: Voltage Inversion Technique to Ascertain Malicious Insertions in ICs	104
<i>M. Banga, M. S. Hsiao</i>	
Dynamic Evaluation of Hardware Trust	108
<i>D. McIntyre, F. Wolff, C. Papachristou, S. Bhunia, D. Weyer</i>	
Author Index	